

Calculating Availability – Environmental Faults

April 2007

In our previous six issues, we have looked at the impact of various strategies and failure mechanisms on the availability of a redundant system. These have included:

- the impact of redundancy
- the impact of repair strategies
- the impact of node recovery and system restore times
- the impact of continuing improvements in hardware reliability
- the impact of failover time
- the impact of failover faults

System outages are caused by many factors, including hardware failure, software bugs, operator errors, and environmental problems. We have considered all of these factors in our previous articles except for the impact of environmental faults. In this article, we complete our analysis of availability by considering faults due to such events as power, fire, flood, earthquakes, hurricanes, social unrest, and malicious acts.

Availability Review

To pick up where we left off, we had developed the following availability relationship for a redundant system with a single spare and with parallel repair:¹

$$\begin{aligned}
 F \approx & \frac{r/2 + R}{r/2} \frac{n(n-1)}{2} (1-a)^2 && \text{hardware/software faults with parallel repair} \\
 & + \frac{\text{MTFO}}{r} n(1-a) && \text{failover time} \\
 & + p \frac{R}{r} n(1-a) && \text{failover faults}
 \end{aligned} \tag{1}$$

where

- F is the probability that the system will be unavailable.
- r is the time required to return a node to service (hardware repair time plus node recovery time).
- R is the time to restore the system to service once a node has been recovered.
- n is the number of nodes in the system.
- a is the availability of a node.
- MTFO is the mean time to fail over from a failed node to an operable node.

¹ Environmental faults are analyzed in more detail in Chapter 2, [Reliability of Distributed Computing Systems](#), *Breaking the Availability Barrier: Achieving Century Uptimes with Active/Active Systems*, AuthorHouse: 2007.

p is the probability that a failover will fail (a failover fault).

This relationship gives the probability that the system will be unavailable to its users. It covers the cases in which two nodes in the singly-spared system fail due to a hardware or software failure or due to an operator error, thus taking down the system; in which one node has failed and the system is unavailable while it fails over to a spare node; and in which a failover attempt fails. It assumes parallel repair. This means that each failed node is being worked on independently to return it to service. That is, there are repair personnel at each failed site.

If there is only one repair person to service all failures, only one node at a time will be worked on. This is the case of sequential repair. In this case, the factors of 1/2 disappear in the first term of the above relationship.

The case of multiply-spared systems is considered in our first article in this series. Entitled [Calculating Availability – Redundant Systems](#), it was published in the *Availability Digest* issue of October, 2006. If there are multiple spares in the system, the first term is modified as shown in that article.

Asymmetric Availability

We normally think of a redundant system as a network of like nodes. In our relations, we have represented the availability of a node by the symbol a .

However, this changes when we consider environmental faults. Though the system in Florida may be identical to the system in Idaho, the real availabilities of these systems may be quite different. It is not unlikely that the Florida system will be taken down by a hurricane. However, it is much less likely that the system in Idaho will suffer an outage due to a natural disaster (a prairie fire, perhaps). If we accept this, over the long run the Florida system will be down more often than the Idaho system and therefore will have a lower availability.

Thus, by considering environmental faults, we are now faced with asymmetric availabilities throughout the application network. Each node has a different availability, and our availability relationships must be modified to accommodate this.

Calculating Nodal Availability with Environmental Faults

To calculate the availability of a node that may experience environmental faults, we must first evaluate the effect of each kind of environmental fault. This means that we must estimate the probability that each fault may occur and how long the system will be down should that sort of fault occur. Since environmental faults are generally few and far between, this is at best an inexact science. However, reasonable guesses can be made; and parameters can be modified to play “what-if” games.

Let us define the following terms for a particular node in the system:

a_i	Is the availability of node i .
f_i	is the probability of node failure of node i .
$mtbf$	is the mean time before failure of the node due to a system fault (hardware, software, operator error).
mtr	is the mean time to recover the node following a system fault.
$mtbe$	is the mean time between failure of the node due to an environmental fault.
$mtre$	is the mean time to recover the node following an environmental fault.

The probability that the node will be down due to a system fault is

$$\frac{mtr}{mtbf + mtr} \approx \frac{mtr}{mtbf}$$

Likewise, the probability that the node will be down due to an environmental fault is

$$\frac{mtre}{mtbe + mtre} \approx \frac{mtre}{mtbe}$$

Thus, the probability of failure of the node i , f_i , is

$$f_i \approx \frac{mtr}{mtbf} + \frac{mtre}{mtbe}$$

and

$$a_i = 1 - f_i$$

If there are several environmental faults of concern, the probability of nodal failure due to an environmental fault is the sum of the individual failure probabilities, $mtre/mtbe$.

As an example, let us consider a node with a system mtbf of 4000 hours (about six months) with an mtr of four hours. This system therefore has a failure probability of $4/4000 = .001$ (three 9s).

Now let us consider environmental faults. Let us assume that the system will be taken out once every ten years (3652 days) by a hurricane and will require one day to return it to service. Furthermore, it will experience an area power failure about once every 8,000 hours (about once per year); and the backup diesel power system will fail once every ten times, resulting in a node failure due to a power outage once every 80,000 hours. When the power backup system fails, it will take 8 hours to bring the system back into service. Therefore, the probability of failure due to an environmental fault is

$$\frac{1}{3,652} + \frac{8}{80,000} = .00038$$

and the nodal failure probability is $.001 + .00038 = .00138$. The node availability has been reduced from .999 to .99862. Environmental faults have added over one third to the system downtime.

Two-Node Systems

Given a proper calculation of the availability for each node, a calculation which takes into account environmental faults, our previous analysis holds. Let us consider a two-node system with availabilities of a_1 and a_2 , respectively.

Dual Node Failure

The probability that both nodes will fail is $(1-a_1)(1-a_2)$. Given a node recovery time of r and a system restore time of R , the first term in Equation (1), which gives the probability that the system will be down due to a dual node failure, becomes

$$\frac{r/2 + R}{r/2} (1-a_1)(1-a_2)$$

Failover Times

Likewise, we can adjust the expression for failover time. A failover will occur whenever a single node fails. In our previous analysis, we noted that an n node system in which each node has an availability of a will experience a node failure with a probability of $n(1-a)$. In our current example, the probability that node 1 will fail is $(1-a_1)$; and the probability that node 2 will fail is $(1-a_2)$. Therefore, the probability of a single node failure is $(1-a_1) + (1-a_2)$, or $(2-a_1-a_2)$; and our previous expression for system downtime during failover given by the second term in Equation (1) becomes

$$\frac{\text{MTFO}}{r}(2-a_1-a_2)$$

Failover Faults

A failover fault occurs with a probability of p whenever a failover occurs, which, as argued above, will occur with a probability of $(2-a_1-a_2)$. Therefore, the third term in Equation (1), which gives the probability of system downtime due to a failover fault, becomes

$$p\frac{R}{r}(2-a_1-a_2)$$

System Downtime

The resulting probability of the system being down when environmental faults are considered is the sum of the above three terms:

$$\begin{aligned} F \approx & \frac{r/2+R}{r/2}(1-a_1)(1-a_2) && \text{hardware/software faults with parallel repair} \\ & + \frac{\text{MTFO}}{r}(2-a_1-a_2) && \text{failover time} \\ & + p\frac{R}{r}(2-a_1-a_2) && \text{failover faults} \end{aligned} \quad (2)$$

Active/Active Systems

As we saw in our previous analyses, if an n -node redundant system is active/active, only $1/n$ of the users are affected by failover times and failover faults. Therefore, these terms in Equation (2) should be divided by a factor of 2 ($n = 2$) for a two-node active/active system.

N-Node Systems

Equation (2) can be extended to an n -node system with a single spare. The downtime expression for this case becomes

$$F \approx \frac{r/2+R}{r/2} \frac{1}{2} \sum_i \sum_{j \neq i} (1-a_i)(1-a_j) + \frac{\text{MTFO} + pR}{r} \left(n - \sum_i a_i \right) \quad (3)$$

The $\frac{1}{2}$ factor before the double summation sign is needed because the double summation adds each pair twice.

Again, if the redundant system is active/active, the last term for the system downtime due to failover time and failover faults should be divided by n since only $1/n$ users are affected.

A Caveat

In the above equations, we have assumed that the time to return a node to service, r , is the same for all nodes. If this is not the case, then the factor $(r/2+R)/(r/2)$ must be modified. The correct value can be determined by analyzing the state diagram for the particular configuration.²

Summary

We have extended our availability equations to include the possibility of natural and manmade disasters which can take down a system. The effect of such environmental faults is to reduce the availability of a node.

If the nodes are geographically dispersed, it is likely that each will be subject to a different set of environmental hazards. Therefore, the various nodes will exhibit different availabilities. The modification of the availability relationships to account for environmental faults takes into account this availability heterogeneity.

The modified relationships extend beyond environmental faults to any set of nodes whose availability characteristics are different from each other. For instance, this analysis can be applied to processing networks in which the nodes are configured differently or are from different vendors.

² See Appendix 3, [Failover Fault Models](#), *Breaking the Availability Barrier: Survivable Systems for Enterprise Computing*, AuthorHouse; 2004, for examples of this sort of analysis.